



Insper

# **Ativos Digitais e Blockchain**

**Ricardo Rocha**  
**Raul Ikeda**

# Objetivo

- Introdução à tecnologia Blockchain

# Blockchain

- O que é Blockchain?
  - Em poucas palavras: um banco de dados NoSQL descentralizado.
- Vantagens:
  - Auditável
  - Imutável
  - Robusto
  - "Democrático"
- Desvantagens:
  - Baixa performance
  - "Hackeável" (e de várias formas)
- Video Explicativo: [https://youtu.be/SSo\\_ElwHSd4](https://youtu.be/SSo_ElwHSd4)

# Blockchain – Quando usar

Pense na sua solução e nas partes envolvidos, respondendo as seguintes perguntas:

- Os recursos e/ou dados são compartilhados entre as partes?
- Sua solução precisa de um intermediário para auditoria?
- Há problemas de confiança entre as partes envolvidas?
- Você abre mão de desempenho computacional?
- Você não precisa de uma solução distribuída?
- Está disposto a pagar mais caro que uma solução tradicional?

Se você respondeu **SIM** a todas as questões, estaria elegível a utilizar Blockchain como plataforma da solução.

Se as informações precisam ser públicas, utilize Blockchain Pública, senão utilize Blockchain Privada.

# Origens

- Bitcoin: A Peer-to-Peer Electronic Cash System – Nakamoto S.
- Ideia: criar uma forma de transacionar valores eletronicamente e descentralizado que evitasse o *double spending*.
- Junção de várias técnicas já conhecidas: peer-to-peer, lista ligada, hash function, private/públic key, etc.
- Continuação do trabalhos:
  - "How to Time-Stamp a Digital Document", Haber & Stornetta, 1991.
  - "Pricing via Processing or Combatting Junk Mail", Dwork & Naor, 1993.
  - "Proofs of work and bread pudding protocols", Jakobsson & Juels, 1999.
  - "Reusable Proof-of-Work", Finney, 2014.
  - "Hashcash - a denial of service counter-measure", Back, 2002.

# Tecnicamente:

## Hash Function: Exemplo SHA256

### SHA256 Hash



A screenshot of a web-based SHA256 hash calculator. The interface has a light gray background. On the left, there is a vertical gray bar. To its right, there are two input fields. The top field is labeled 'Data:' and contains the text 'Exemplo de Hash dos dados'. The bottom field is labeled 'Hash:' and contains the long alphanumeric string 'f30cead3aabf926b8f14d3e2bcf7f7d376a4d540516e005efd47f7d91f3b289c'. This bottom field is highlighted with a red rectangular border.

Label	Value
Data:	Exemplo de Hash dos dados
Hash:	f30cead3aabf926b8f14d3e2bcf7f7d376a4d540516e005efd47f7d91f3b289c

Mais detalhes: <https://pt.wikipedia.org/wiki/SHA-2>

# "Mineração"

Calcular o **nonce** cujo o resultado do hash comece com n zeros.

Block

Block: # 1

Nonce: 19905

Data: Alguns dados aqui

Hash: a09687d911736444ec57a3222c5651c2dff1a92bd9a8002a0df3ced0dba03131

Mine

Block

Block: # 1

Nonce: 3856

Data: Alguns dados aqui

Hash: 00002180a881c52c46020f8ee354e73c71d06bfc962027999a8d9407b1a22693

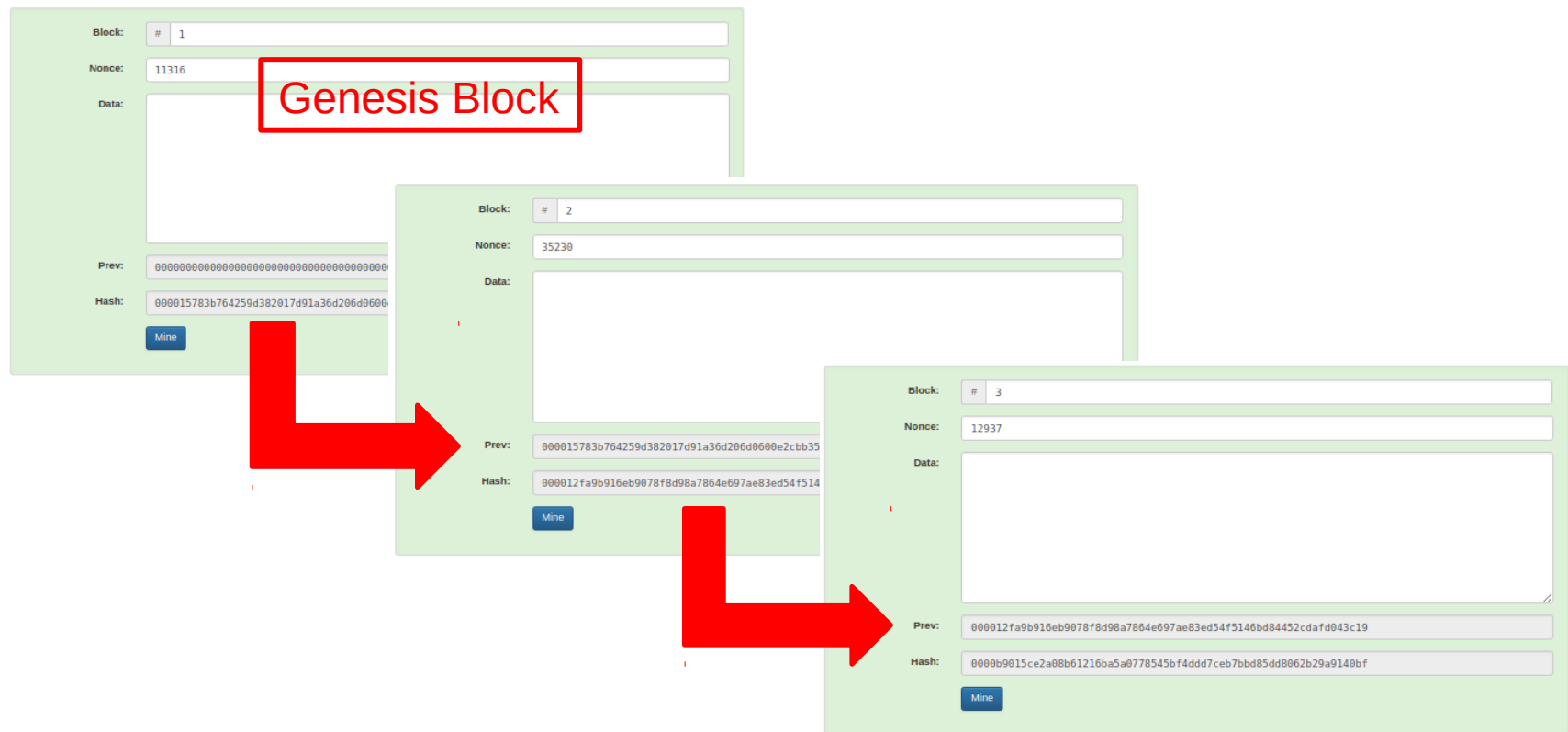
Mine

Dúvida: Existe apenas um nonce possível?

# Blockchain

1. Lista ligada de blocos: O hash do bloco atual é formado pelo hash anterior + dados do bloco + nonce.

## Blockchain





Pulo do gato: Se alterar algo em algum bloco, o seu hash seria alterado. Minerando novamente o bloco, dificilmente o hash se manteria o mesmo. Logo a lista se tornaria inconsistente.

## Blockchain

Block: #	Nonce	Data	Prev	Hash
1	6813	1	00	000073e74b79801c339a3eb9155e87eebe201205575a159dc293bed948
2	38033	2	000073e74b79801c339a3eb9155e87eebe201205575a159dc293bed948	0000f60d1de0cad586f3e9aa5c69d03c50ab87735628429941e32bfdb0
3	21689	3	0000f60d1de0cad586f3e9aa5c69d03c50ab87735628429941e32bfdb0	0000755687a60cfba13fda52b69d54cf290

## Blockchain

Block: #	Nonce	Data	Prev	Hash
1	6813	1	00	000073e74b79801c339a3eb9155e87eebe201205575a159dc293bed948
2	121409	ABCD	000073e74b79801c339a3eb9155e87eebe201205575a159dc293bed948	00006221a84772a93c95e82d8a04b937f8231f1d5cfffbb946259cb2c85
3	21689	3	00006221a84772a93c95e82d8a04b937f8231f1d5cfffbb946259cb2c85	99b03cc9f3c9d04013e9d06b5bc50bd87c

# Transações

E se os dados contidos no bloco representassem transações financeiras entre duas partes:

**Block:**

**Nonce:**

**Tx:**

\$	25.00	From:	Darcy	->	Bingley
\$	4.27	From:	Elizabeth	->	Jane
\$	19.22	From:	Wickham	->	Lydia
\$	106.44	From:	Lady Catheri	->	Collins
\$	6.42	From:	Charlotte	->	Elizabeth

**Prev:**

**Hash:**

Como garantir que a transação realmente partiu da conta origem?

# Transações

Assinatura: Chave pública e privada.

A origem e destino não precisa necessariamente ser identificado nominalmente:

Block:

# 3

Nonce:

29164

Coinbase:

\$ 100.00 -> 04fe1be031bc7a54d900ff06291

Tx:

\$ 10.00 From: 04222d7af343ab -> 04d4080959e3795

Seq: 1 Sig: 30450220485a5a1c317d5a1b33af90201999909b49e09dc5

\$ 5.00 From: 041c377677bb697 -> 04d4080959e3795

Seq: 1 Sig: 3044022002cc3c61bb7cd4573b192d1b61f125545ebc84c5

\$ 20.00 From: 04997ac426a5c3c -> 040b4c84f02bfec

Seq: 1 Sig: 3045022100ee33bb3764f5f85f694d1033a66131bc818c18

Prev:

00008ccb2fccac084b800a2878d317e14fe88fddb1e91d131d1fc3d523d67125

Hash:

000029942f0286f943ac7e877d7f10c3902aecbb2eebc72a758ab40487b0b8f9

Mine

Insper

# Consenso e Votação

- Para evitar fraudes, cria-se uma rede *peer-to-peer*, onde cada nó possui uma cópia do Blockchain.
- Quando um novo nó é minerado, envia-se os dados do bloco a todos os nós da rede.
- Cada nó declara se aceita ou rejeita o bloco em questão. Caso um certo número de nós aceite o bloco, ele é incorporado ao Blockchain e começa-se a minerar um novo bloco.
- Durante a análise do bloco, os nós também avaliam a validade dos dados, e no caso de transações financeiras, se haveria saldo suficiente para efetuar cada transação.
- Caso o nó enviado seja inválido, se o minerador insistir em incorporar o bloco, ele irá divergir do resto da rede (fork).

# Coinbase

- Equilíbrio do jogo: Qual o incentivo dos nós para minerar e manter uma cópia dos dados? Isso custa dinheiro.
- Ideia do Bitcoin: cada bloco minerado atribui um certo valor para a conta do minerador. Ainda, cada transação registrada paga um valor para o minerador do bloco.
- Dúvida: É possível haver um Blockchain sem uma moeda atrelada?

# Forking

- O que acontece se dois mineradores acharem o bloco ao mesmo tempo?
- Como em um sistema de "votação" quem obter a maioria dos nós reconhecendo o bloco, venceria o pleito. Durante a divergência, cada nó cria um fork na lista e vai empilhando. Quando o consenso é atingido, descarta-se o ramo preterido.
- No caso extremo, pode haver cisão e haver duas redes diferentes. Em alguns casos o fork é intencional (troca de configuração, divergências permanente entre nós, etc).